1 CLAIMS

2 We claim:
3 1. An information distribution system comprising:

4   a key management server for managing secret keys and
5   public keys corresponding to given attribute values;

6   a user terminal for accessing said key management
7   server to obtain attribute secret keys generated based
8   on said secret keys, said attribute secret keys
9   corresponding to attributes of said user terminal; and

10   a provider terminal for generating an encrypted
11   content that can be decrypted by said user terminal
12   having said attribute secret keys corresponding to
13   given attributes by means of said public keys,

14 wherein said provider terminal distributes said encrypted
15 content and said user terminal decrypts said encrypted
16 content decryptable by means of said attribute secret keys
17 of its own.

18 2. The information distribution system according to claim 1,
19   wherein said provider terminal distributes said
20   encrypted content without specifying said user
21   terminal that is to receive said encrypted content.

22 3. The information distribution system according to claim 1,
23   wherein said user terminal sends a set of attribute
24   values indicating attributes of its own to said key
25   management server; and

1	said key management server generates said attribute
2	secret keys unique to said user terminal based on,
3	among said secret keys managed by said key management
4	server, secret keys corresponding to the attribute
5	values sent from said user terminal and sends said
6	attribute secret keys to said user terminal.

7 4. A server comprising:

8   a key storage for storing secret keys and public keys
9   corresponding to predetermined attribute values;

10   an attribute secret key generator for obtaining a set
11   of given attribute values and generating attribute
12   secret keys corresponding to said set of attribute
13   values based on secret keys corresponding to said
14   attribute values among said secret keys stored in said
15   key storage; and

16   a sending/receiving unit for receiving said set of
17   attribute values from a given user terminal and
18   sending said attribute secret keys generated by said
19   attribute secret key generator to said user terminal.

20 5. The server according to claim 4, wherein said attribute
21   secret key generator generates said attribute secret
22   keys by using a protocol implementing oblivious
23   transfer.

24 6. An information processing apparatus comprising:

25   a criteria key generator for obtaining public keys
26   corresponding to attribute values indicating

1   attributes of a recipient to which a content is to be
2   sent and using said public keys to generate criteria
3   keys that can be decrypted by secret keys
4   corresponding to said public keys;

5   an encrypted content generator for encrypting said
6   content based on said criteria keys; and

7   a sending unit for sending said encrypted content
8   without specifying any recipient of said content via a
9   network.

10   7. The information processing apparatus according to claim
11   6, wherein said criteria key generator combines, based
12   on predetermined rules, criteria keys corresponding to
13   the individual attribute values encrypted by using
14   public keys corresponding to said individual attribute
15   values to generate a criteria key for restricting
16   recipients of said content.

17   8. The information processing apparatus according to claim
18   6, wherein said criteria key generator generates a
19   session key for encrypting said content and a criteria
20   key for decrypting said session key; and

21   said encrypted content generator uses said session key
22   to encrypt said content.

23   9. An information processing apparatus receiving a content
24   distributed over a network, comprising:

25   a sending/receiving unit for accessing a key
26   management server managing secret keys and public keys

1 corresponding to given attribute values to receive
2 attribute secret keys corresponding to attributes
3 established for said information processing apparatus,
4 said attribute secret keys being generated based on
5 said secret keys; and

6 a decryptor for obtaining an encrypted content and
7 decrypting said content based on said attribute secret
8 keys.

9 10. The information processing apparatus according to
10 claim 9, wherein said sending/receiving unit sends a
11 set of attribute values established for said
12 information processing apparatus to said key
13 management server and receives said attribute secrete
14 keys generated based on said set of attribute values
15 from said key management server.

16 11. A program for controlling a computer to generate a
17 decryption key for decrypting information encrypted
18 with a given public key, said program causing said
19 computer to implement the functions of claim 4.

20 12. The program according to claim 11, wherein said
21 computer-implemented function of generating said
22 attribute secret key generates said attribute secret
23 keys by using a protocol implementing oblivious
24 transfer.

25 13. A program for controlling a computer to encrypt and
26 distribute a given content, causing said computer to
27 implement the functions of claim 6.

1   14.   The program according to claim 13, wherein said
2   computer-implemented function of generating said
3   criteria key combines, based on predetermined rules,
4   criteria keys corresponding to the individual
5   attribute values encrypted by using public keys
6   corresponding to said individual attribute values to
7   generate a criteria key for restricting recipients of
8   said content.

9   15.   A program for controlling a computer to receive
10   content distributed over a network, causing said
11   computer to implement the functions of:

12   accessing a key management server managing secret keys
13   and public keys corresponding to given attribute
14   values to receive attribute secret keys corresponding
15   to attributes established for said information
16   processing apparatus according to claim 6, said
17   attribute secret keys being generated based on said
18   secret keys; and

19   obtaining the encrypted content and decrypting said
20   encrypted content based on the attribute secret keys.

21 16.   A storage medium containing a program in computer
22   readable form for controlling a computer to generate
23   decryption key for decrypting information encrypted
24   with a given public key, said program causing said
25   computer to implement the functions of claim 4.

26 17.   A storage medium containing a program in computer
27   readable form for controlling a computer to encrypt
28   and distribute a given content, said program causing

1   said computer to implement the functions of claim 6.

2   18.   A storage medium containing a program in computer
3   readable form for controlling a computer to receive a
4   content distributed over a network, said program
5   causing said computer to implement the functions of
6   claim 9.

7   19.   A key distribution method for controlling a computer
8   to generate and distribute a decryption key for
9   decrypting information encrypted with a given public
10   key, comprising the steps of:

11   generating n secret keys and n public keys
12   corresponding to said secret keys and storing said
13   secret keys and public keys in a given storage;

14   obtaining information about k ($\leq$n) secret keys
15   selected at random by a given client from among said n
16   secret keys stored in said storage;

17   reading said k secret keys corresponding to
18   information about the obtained secret keys from said
19   storage and using a protocol for implementing
20   oblivious transfer to generate decryption keys for
21   decrypting information encrypted with said k public
22   keys corresponding to the k secret keys; and

23   providing said generated decryption keys to said
24   client.

25   20.   An information distribution system comprising:

1 a service provider managing secret keys and public
2 keys for given attribute values; and

3 a plurality of user terminals for accessing said
4 service provider to obtain attribute secret keys
5 corresponding to attributes of their own, said
6 attribute secret keys being generated based on said
7 secret keys;

8 wherein, a given one of said user terminals generates
9 an encrypted content and sends said encrypted content
10 to one or more of the other user terminals, said
11 encrypted content being decryptable by said one or
12 more of the other user terminals having said attribute
13 secret keys corresponding to given attributes by means
14 of said public keys; and

15 said one or more of the other user terminals decrypt
16 said encrypted content decryptable by means of said
17 attribute secret keys of their own.

18 21. An information distribution system comprising:

19 a key management server for managing secret keys and
20 public keys for given attribute values; and

21 a plurality of user terminals for accessing said key
22 management server to obtain attribute secret keys
23 corresponding to attributes of their own, said
24 attribute secret keys being generated based on said
25 secret keys,

26 wherein a given one of said user terminals generates a group

1   key and sends said group key to ones of the other user
2   terminals and provides a content , said encrypted group key
3   being decryptable by said ones of the other user terminals
4   having said attribute secret keys corresponding to given
5   attributes by means of said public keys, said content being
6   only accessible by using said group key.

7   22. An article of manufacture comprising a computer usable
8   medium having computer readable program code means embodied
9   therein for causing key distribution, the computer readable
10   program code means in said article of manufacture comprising
11   computer readable program code means for causing a computer
12   to effect the steps of claim 19.

13   23. A program storage device readable by machine, tangibly
14   embodying a program of instructions executable by the
15   machine to perform method steps for key distribution, said
16   method steps comprising the steps of claim 19.

17   24. A computer program product comprising a computer usable
18   medium having computer readable program code means embodied
19   therein for causing key distribution, the computer readable
20   program code means in said computer program product
21   comprising computer readable program code means for causing
22   a computer to effect the functions of claim 20.

23   25. A computer program product comprising a computer usable
24   medium having computer readable program code means embodied
25   therein for causing key distribution, the computer readable
26   program code means in said computer program product

1   comprising computer readable program code means for causing

2   a computer to effect the functions of claim 21.